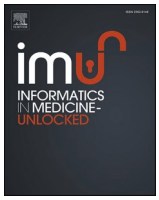
Informatics in Medicine Unlocked 30 (2022) 100903

Contents lists available at ScienceDirect

Informatics in Medicine Unlocked

journal homepage: www.elsevier.com/locate/imu



AI-driven IoT for smart health care: Security and privacy issues

Ismail Keshta

Computer Science and Information Systems Department, College of Applied Sciences, AlMaarefa University, Riyadh, Saudi Arabia

ARTICLE INFO

Keywords:
IoT
AI
AIIoT
Health care
Privacy, and security

ABSTRACT

The Internet of Things (IoT) has recently brought the dream of a smarter world into an accurate picture with various services and a significant amount of data. With the innovation of smart Multiple Sensorial Media (MulSeMedia) systems, the cloud, and things technologies, "smart health care" is receiving considerable attention from health care communities, industry, government, and academia. The purpose of the present research has been to establish the AI-driven IoT (AIIoT) security and privacy issues and recommend the manner in which all such matters can be adequately addressed. The study employed a qualitative study design in which qualitative information was collected from existing relevant secondary sources. The evidence from the findings shows that the evolution of AI-driven IoT (AIIoT) has added to the significant number of new sensors and devices to the internet, creating an assortment of security and privacy concerns among the users. The study recommends that the current requirement for the AI-driven IoT (AIIoT) is to have certain types of well-defined architecture standards that include interfaces and data models that ensure that the privacy and security of the users are enhanced.

1. Introduction

With the innovation of smart multiple sensorial media (MulSeMedia) systems, the cloud, and things technologies, "smart health care" is receiving significant attention from health care communities, industry, government, and academia. The Internet of Things (IoT) has recently brought the dream of a smarter world into an accurate picture with many services and a significant amount of data [1]. With the outbreak of the COVID-19 pandemic, artificial intelligence (AI) has equally gained a substantial amount of attention by using its machine learning algorithms for providing quality care to patients. However, the literature points out that the convergence of AI and IoT can offer new opportunities for the two technologies. AI-driven IoT can play a very important role in smart health care by providing better insight into specific health care data to support affordable and quality personalized care [2]. AI-driven IoT might equally support powerful storage and processing facilities of large amounts of IoT data streams beyond the ability of the individual "things" to provide automated medical decision-making in real time. While scholars have advanced their studies of AI and IoT for health care services, little attention has been placed on the security and privacy issues associated with such devices. The AI-driven IoT (AIIoT) for smart health care is able to revolutionize a number of aspects within the health care industry; however, a number of technical concerns must be addressed before such potential is achieved [3].

The purpose of this research is to outline AI-driven IoT (AIIoT) security, including authentication, access control, security models, and privacy issues. With the vast number of devices connected to the internet and the greater quantity of data linked with those connections, there has always been a significant concern in related security issues that surround the Internet of Things. The present essay addresses AI-driven IoT (AIIoT) security in smart health care and medical devices. Specifically, the essay presents an analysis of what constitutes IoT security, the unique and common AI-driven IoT (AIIoT) security issues in comparison with network and information or traditional cybersecurity, the different approaches for IoT security, and the types of security measures that should be taken in addressing AI-driven IoT (AIIoT) security issues. Scholars argue that since AI-driven IoT (AIIoT) is very much associated with information technology and communication, it is prudent to consider privacy and security challenges that are already known within information security and examine how all these are transferred into the present and future state of AI-driven IoT (AIIoT) [4]. While the literature affirms that some characteristics make privacy and security challenges in the AI-driven IoT (AIIoT) very much distinct, limited studies have investigated the real privacy and security issues associated with the IoT in health care. A deeper investigation on the matter is needed. This finding informs the reason why the present research will be of great benefit. Therefore, this paper presents an overview of the challenges and concerns of AI-driven IoT (AIIoT) for smart health care while convergent

E-mail address: imohamed@mcst.edu.sa.

https://doi.org/10.1016/j.imu.2022.100903
Received 10 August 2021; Received in revised form 21 February 2022; Accepted 5 March 2022
Available online 14 March 2022

on smart health care systems.

1.1. Broad objectives

To present an overview of the security, privacy, and trust challenges and concerns of AI-driven IoT (AIIoT) for smart health care convergent systems.

1.2. Specific objectives

The present essay seeks to achieve the following specific objectives:

a. To identify security, privacy, and trust challenges and concerns of AI-driven IoT (AIIoT) for the smart health care systems.
b. To outline the type of security, privacy, and trust measures that should be taken when applying AI-driven IoT (AIIoT) for smart health care systems.

2. Materials and methods

2.1. Study design

The present study did develop a systematic review of secondary literature in relation to the study topic. A good research study is one that has the ability to access secondary data from an appropriate source and make use of the information. According to Smith et al. [5], a vast amount of information has been archived over the years. Therefore, it is practical to utilize existing data and information to conduct secondary research. Crowther et al. [6] argue that secondary data analysis involves analyzing and interpreting data collected by another researcher for another purpose. This approach is a viable research method that is less costly and saves on time spent going to the field for data collection. This method was proposed for this study because it considers the resources and time available to the researcher. Si et al. [7] argue that secondary data are accessed easily and help to define the problem better and have clear insight and understanding into the problem to help formulate and apply interventions. The current study ensures that the information used was current, relevant to the study, and accurate.

2.2. Sampling procedure

A sampling process of the secondary literature involved selecting secondary data that were accessible online and had some relevancy to matters about security, privacy, and trust challenges and concerns of AI-driven IoT (AIIoT) for smart health care convergent systems. For any given article to be chosen as a sample within this study, it had to be specific to the AI-driven IoT (AIIoT), emphasizing security (authentication, access control, security models) and privacy concerns, even more within smart health care centers. For the other thesis studies and scholarly review articles, the study was picked for review in this study only if it met the inclusion criteria that had already been written.

In other words, the study had been conducted to identify specific security and privacy risks associated with AI-driven IoT (AIIoT), data had been generated from very reliable sources, or random sampling had been applied in the collection of such data, among other things. Data that had been collected through random sampling were offered first priority during the process of systematic review due to the many advantages that randomization enjoys over the other methods of data collection, such as nonrandomized sampling, which in the majority of cases always have some form of business.

A systematic literature review was one of the most effective methods that could be applied in the general analysis of the matters pertaining to security, privacy, and trust challenges and the concerns of AI-driven IoT (AIIoT) for smart health care convergent systems. Abstracts and titles of all of the links that had been selected were checked first, and only the sources of data that appeared to be within the criteria of inclusion had their content generated and the hard copy printed to help in the analysis. The content of all of these sources of data was then scanned to ensure that they were actually related to issues about security, privacy, and trust challenges and the concerns of AI-driven IoT (AIIoT) for smart health care systems, and second, the type of security, privacy, and trust measures that should be taken when applying AI-driven IoT (AIIoT) for smart health care systems. No other thing was accepted except for the literature that contains the content required in the study objective.

Additionally, more evaluation was performed on all of the selected sources to ensure that they were very appropriate for inclusion in the review. The critical questions used in the evaluation comprised whether the article or journal had adequately addressed the broad objective of the study. The validity of the information source was also given some consideration to confirm whether the arguments in the books and articles would be relevant to the risks posted by the AI-driven IoT (AIIoT) and to what extent the security and privacy risks could be addressed.

2.3. Data collection process

The literature search was performed to establish instances of privacy and security breaches in the application of AI-driven IoT (AIIoT) in smart health care. Appropriate secondary sources for review included journal articles, books, and periodicals on security, privacy, and trust challenges and concerns of AI-driven IoT (AIIoT) for smart health care convergent systems. The university library database was used to find books and other scholarly articles. Each article was generated by first entering relevant keywords into databases within computer systems. The researcher made a search of different peer-reviewed articles from various databases, which included Google Scholar, EBSCOhost, ERIC, and Academic OneFile. Different keywords were used in making the search. Words such as 'Information Security Culture', 'privacy', 'AI-driven IoT′, and 'Smart health care" were used in the search process. The articles and papers were selected from the above search results based upon reference to an approach or a set of recommendations for addressing security, privacy, and trust challenges and concerns of AI-driven IoT (AIIoT) for smart health care convergent systems.

The search strategy applied in a number of organization databases reflects 5000 records, which also comprise the conventional research studies and other health institutions' reports. Despite having substantial amounts of data accessible through the search strategy, a data cleaning process was heavily applied, removing all duplicates. After removing all of the duplicates, 2,135, the titles and abstracts of the remaining 2865 articles were reviewed. A further 2500 were excluded because they did not meet the inclusion criteria. Furthermore, no study on "ongoing review" was included. Other studies were excluded based on design and general research methodology. The PRISMA study flowchart, Fig. 1 below, illustrates the search results.

2.4. Data synthesis and analysis

Both ongoing and recursive data analysis approaches were applied to analyze the qualitative data. The literature by James et al. [8] has always indicated that there are two main strategies for analysis: holistic and categorical analysis. The researcher opted for categorical analysis in analyzing the qualitative data in this paper. It is essential to mention that categorical analysis involves coding as well as sorting out of data into categories that had already been established, while the holistic approach, on the other hand, involves given programs, situations, and experiences. The literature clarifies that the holistic approach is primarily based on narration and description. To enhance qualitative analysis, researchers are encouraged to apply both holistic and categorical analysis. While Tealab [9] argues that ethnographers can always gather data through artifacts, interviews, and physical observation, the qualitative data used in this paper mainly came from documents and systematic reviews of existing scholarly literature. The study was not focused on qualitative data.

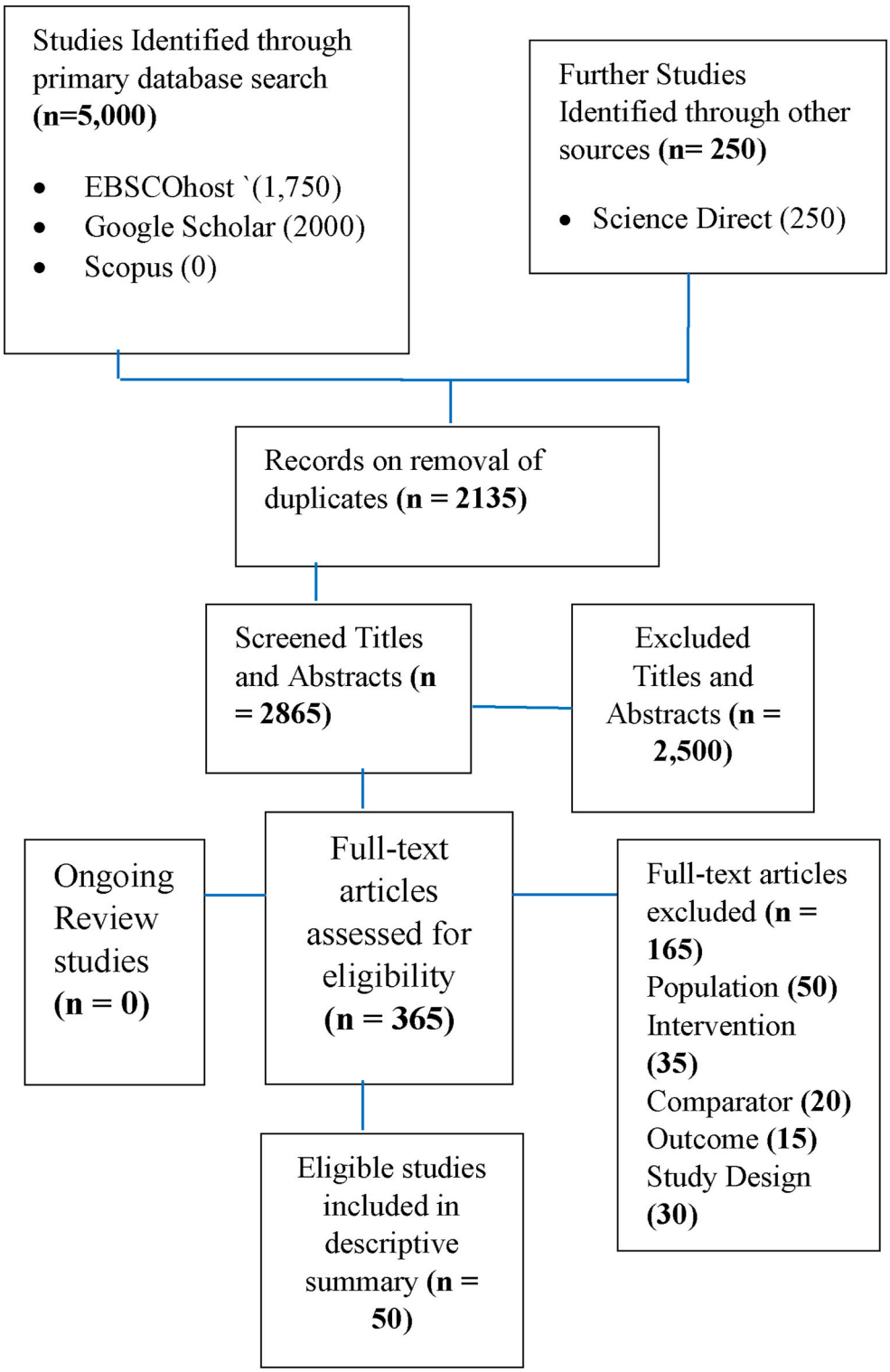


Fig. 1. PRISMA study flowchart of search results.
Source: Author's own generation

The present study's main focus was on assessing matters that pertain to security, privacy, and trust challenges and the concerns of AI-driven IoT (AIIoT) for smart hospitals and medical devices. Therefore, a permutation of all-inclusive and definite strategies was somewhat critical, because the researcher would analyze qualitative data from secondary literature through the categorical strategy. The categories developed in this case would guide further analysis processes. For the purpose of portraying the perceptions of the examined literature on security and privacy risks associated with the AI-driven IoT (AIIoT), the application of holistic analysis was found by the researcher to be of more importance immediately after developing categories since the researcher narrated the literature findings that pertained to security, privacy, and trust challenges and the concerns of AI-driven IoT (AIIoT) for smart hospitals. As indicated in Munn et al. [9], these two strategies for analysis are not

exclusive to each other. The researcher, therefore, applied them together to assist in the analysis of the qualitative data.

2.5. Ethical considerations

The first important ethical issue during the research process was obtaining approvals from the relevant authorities. Second, all of the secondary information that was used in the study was collected with at most good faith and has been properly acknowledged through in-text citation and listing all of the relevant literature within the reference list. The works of other scholars have been appropriately acknowledged to avoid the problem of plagiarism.

3. Findings and discussion

3.1. Usage of the AI-driven IoT (AIIoT) for smart health care convergent systems

The health care sector remains one of the fastest sectors in the world to adopt AI-driven IoT (AIIoT). Integrating AI-driven IoT features into individual medical devices tends to improve the quality and effectiveness of the specific service offered; this approach tends to be very valuable for individual patients who have any form of chronic conditions, elderly individuals, and those who require continuous care. As per the study conducted by Sodhro et al., spending made on health care AIIoT solutions will reach one trillion US dollars by 2025 [10]. It is possible that this situation could help set the stage for having highly accessible, personalized, and on-time health care services for each individual. Fig. 2 illustrates an example of a smart health care system.

Different hospitals have been adopting AI-driven IoT for a number of years. It is very common to witness AI-driven IoT devices in rooms of patients, electronic medical records, and other cloud-based resources. Scholars predict that digital health care will help to revolutionize the whole health care industry by increasing access to diagnosis, preventive care, and treatment and seriously minimizing the relevant costs [12]. Keeping track of patients who are considered to be high risk is a great challenge in keeping down the health care cost. Management of chronic disease is responsible for approximately 30% of the spending on health care in the US, and a more significant proportion of such expenditures is associated with heart disease, diabetes, and asthma.

Artificial intelligence-driven Internet of Things devices such as remote monitoring will make it very possible for health care providers to routinely keep track of high-risk patients. The analysts see the chance of saving up to 350 billion US dollars from digital health care, with more than USD 200 billion of that likely to come from the management of chronic infections, mostly by eliminating wasteful and redundant expenses [13]. The AI-driven IoT can also be described as an artificial intelligence-driven Internet of Medical Things. In such a case, the Internet of Medical Things would be a collection of all medical devices and the corresponding applications that tend to connect to health care information technology systems via a computer network. The Internet of Medical Things, in this case, is medical equipment with Wi-Fi connectivity that tends to communicate with other equipment [13]. Such a group of devices can link with the cloud storage provided by Amazon AWS to store data that have been captured that can later be analyzed.

The literature demonstrates that several areas exist in health care in which the AI-driven IoT can play a crucial role. Examples of such areas are elder care, which involves tracking elderly residence at hospitals and nursing homes and gathering relevant data [11]. It includes several types of equipment that are seen at the bedside within hospitals, such as EKG monitors. This area has continued to expand, with present innovations occurring across the world of AI-driven IoT.

As the usage of AI-driven IoT increases within the health care sector, it is likely to benefit both health care providers and individual patients. Treatments that patients receive are enhanced by remote monitoring and communication, areas within which the AI-driven IoT can play a very large role [11]. The other usage of health care AI-driven IoT is mobile medical applications or wearable devices that make it possible for patients to capture their individual health data. Most of this aspect can be attributed to the data revolution, which empowers the general population to live healthier lives by making good use of connected devices such as wearables, tablets, and hand-held devices (See Fig. 3).

Analysis of the data collected via electronic medical records, the individual diagnostic information collected through imaging equipment and individual handheld devices tend to enhance the power for decision-making [14]. This aspect can allow individual patients to take a very active role in managing their individual personal health. In the future, such data-rich personalized analysis of individual health will be an excellent standard. Patients will be offered tailor-made strategies to help fight illness. From the data generated, people learn in the manner in which they can improve their wellbeing, and they will also be seriously motivated to take control of their individual lives [15]. Scholars argue that there is a new industry within clinical decision support software, a growing sector that is specifically related to AI-driven IoT that boosts the function of the connected devices by using their applications more directly in clinical decisions.

3.2. Security issues in the AI-driven IoT

With the high rate of adopting AI-driven IoT, a very large number of devices are connected to the internet. On a daily basis, such smart objects continue to be on target for their risk to information security [16]. For example, toward the end of 2018, two security scholars discovered more than sixty-eight thousand medical systems that had been exposed

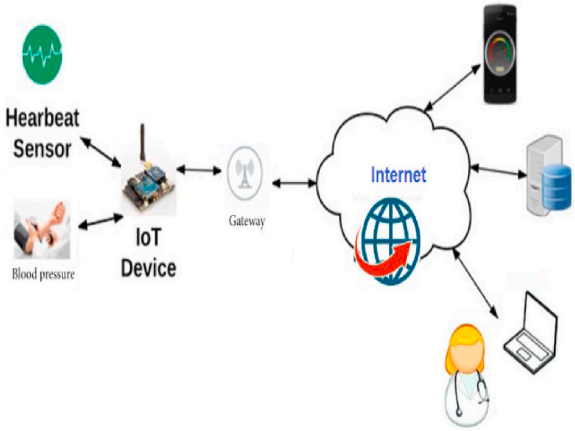


Fig. 2. An example of a smart health care system.
Source [11]

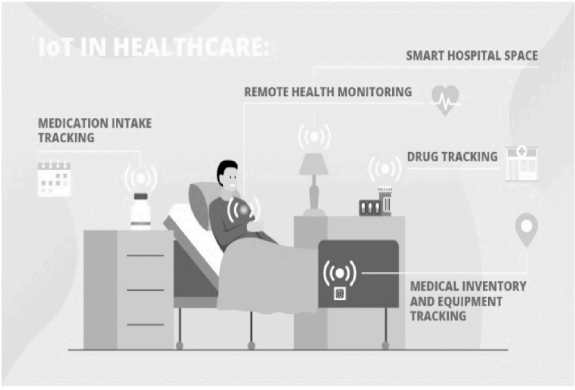


Fig. 3. Illustrating the potential benefits of AI-driven IoT in health care (Fadaeddini 16).

online, and more than 12,000 of them belonged to a single health care organization. One important concern regarding this discovery was that the devices were connected to the internet via computers that were running a very old version of Windows XP, an OS version that is widely understood to pose a large number of vulnerabilities that can be exploited [17]. Such devices were discovered by the use of Shodan, a search engine that is capable of finding AI-driven IoT devices online. These are very easy to hack through a system called brute-force attacks and through the application of hard-coded logins. During the time of their research, the two scientists revealed anesthesia equipment, infusion systems, nuclear medical systems, and simple shodan queries [18]. The researchers, in this case, reported that the attackers did manage to authenticate through SSH on such fake medical devices over 50,000 times, and they even left several malware payloads [19]. The researchers, in this case, also found that in the majority of the cases, the attackers did not realize what they had hacked and left an infected machine behind as part of their individual botnets.

3.3. Privacy threats in the IoT in medical health care

Possible threats in the AI-driven Internet of Things are very difficult to quantify based on the large uncertainties in how and whether the Internet of Things will influence the entire society. On the same note, we can currently observe the impact of the collection of larger quantities of data from smartphone sensors, social media, and mobile network operators [20]. The general implication of the breakthrough of the AI-driven IoT on the aspect of privacy can best be studied based on the experiences of how such technologies tend to be impacted by privacy. By applying this parallel, it can be inferred that even if the data transmitted by a given endpoint device might not result in any issue related to privacy, per se, the amount of data that is accumulated from different devices can also create some types of privacy problems [10]. Additionally, some characteristics tend to make privacy threats to the AI-driven IoT more challenging. The process of collecting data is largely passive, less intrusive, and more pervasive, making the users become minimally aware that they are being tracked. Choi et al. illustrated the IoT components, respective vulnerabilities and threat/attack type, as summarized in Table 1. As illustrated in the table, physical attacks, integrating RFID, integrating WSNS, DOS/DDOS, and unauthorized data access are some of the major threats or vulnerability of IoT components.

Table 1
IoT components, vulnerabilities and threat/attack types in IoT health care applications.

IoT components	Vulnerabilities	Threats/Attack Types
Physical Objects	• Devices of this layer have limited calculation, communication and storage resources	• Physical attacks
	• Nodes are distributed in distant locations; an adversary can easily access the devices and perform damage and illegal actions such as extract security information and keys, reprogram the devices, etc.	• Integrating RFID • Integrating WSNS • DOS/DDOS • Unauthorized data access and access control
Communication Technologies	• Lot is dynamic network infrastructure. • Low power • Lossy network	• Wireless PAN/LAN communications • Wireless WAN communications • Secure lot communication protocols in constrained resources environment
	• The challenges of selection security technique for each element. • Defense capability of the network varies in different networks.	• Secure transmitted data

Source [10]

The literature has acknowledged the fact that AI-driven IoT is pervasive in its general nature, in which case different devices tend to sense and collect data regarding the users as well as their environment to offer some specific type of services. Data that have been collected in this case are processed at the health care service providers, which are situated within the control of the users [12]. Data anonymization, which is always done, that is, replacing personal information with a type of randomly generated distinctive ID, is never sufficient to allow for the anonymity of such users, and it has clearly been demonstrated that the individual identities of the users can be inferred from a group of anonymized datasets. A good example to explain such privacy breaches includes the case of a group of insurance commissions in Massachusetts, which bought health insurance for state employees and released records for every hospital visit by the state employees at no cost to any scholar who wanted such data [13]. To protect the privacy of the patient, the data were specifically anonymized by eliminating fields such as address, name, and social security number, although the ZIP code, gender and birthdate were never removed.

Literature reports that even after eliminating the explicit identifiers from the existing medical data, in a majority of the cases, the remaining part of the data (such as ZIP code, date of birth, and gender) was sufficient to help reidentify individuals when trying to link them with the public voter database [11]. To be more specific, Sweeney could reveal and even send the health records of the governor, including the diagnosis and prescriptions, to his office. The governors assured the general public that such a release of GIC data would not specifically compromise the privacy of the patient [14]. It is important to demonstrate that a serious privacy breach of AOL search data did occur when AOLs released more than 20 million search enquiries using the internet to engage more academic scholars.

AOL had assigned every user a type of unique identification number, although the information, in this case, was very much detailed and personal and one could easily reveal a number of identities of the users and subsequently compromise their individual privacy [14]. The online DVD rental company, Netflix, announced in 2006 a type of open competition to initiate an algorithm that could help improve the recommendation system of its movie by more than 10%. Together with the existing contest, Netflix released a number of training datasets to the existing competitors, including more than 100 million movie ratings, provided by more than half a million users to close to 20,000 movies [15]. The name of the movies and the users, in this case, were replaced by a number of numerical IDs to help anonymize the existing dataset.

Rayan (12) could, however, identify many anonymized Netflix users by making a comparison to the set of data with the individual reviews that were posted on the internet Movie Database [16]. The experiment did show that it was very much possible to identify the political leanings of the users as well as their individual sexual references. This scandal resulted in a lawsuit that was made against Netflix, which subsequently led to the termination of the subsequent round of the contest in 2010 due to concerns about privacy [19]. Within the AI-driven IoT, new technologies, as well as the interconnection of such features and techniques, have magnified the overall threat of being identified.

The use of surveillance camera technology, within the contexts of nonsecurity, is a good example of such relevant techniques, in which case the behaviors of the clients are studied for the purpose of marketing and analysis. In the most recent case scenario, one of the largest drug chain stores in Russia began to apply software for recognizing emotion as a type of pilot test for sensing the facial expression of the customer [19]. The main goal of such technology is to provide a type of customized discount in real time for each individual customer based on how she is feeling and again reviewing her individual purchase history as well as preferences. The automated identification of people from a type of digital image or even a video frame is already being used by the agencies

responsible for law enforcement in several nations.

Speech recognition is very much applied in mobile applications, and a large number of databases of speech samples are already being built, which can possibly be applied to identify and recognize different individuals. The overall increasing interconnection as well as the vertical communication of things tends to open up the chances for making identification of devices by fingerprinting [21]. For instance, it is clearly demonstrated that it is very possible to apply the radio-frequency identification profile of an individual to trace them. To handle such problems, attribute-based authentication is offered to help to minimize communication in AI-driven IoT data and to maintain control over the general disclosure of such data and improve overall user privacy in the AI-driven IoT.

The evolution of the AI-driven Internet of Things has continued to add several billions of new sensors as well as some other devices into the internet, creating a great amount of information in relation to people, including their individual locations, health records, connections, pictures, voices, financial transactions, and conversations, among other items [21]. Surya (17) points out that AI-driven IoT is likely to impact almost everything and every individual in a manner that is not precedented from health care inventions [22]. The AI-driven IoT will be everywhere, which shows that when changes occur, such changes will impact almost everything [17]. However, the author acknowledges that key among the important issues that involves virtuality will be privacy.

The literature identifies tracking and localization as the threats of trying to determine and record the location of a person through time and space using various methods, such as GPS data, internet traffic, and cell phone location [18]. The existence of large amounts of data and detailed spatiotemporal and spatial data, which has become possible as a result of techniques for data collection, such as the global positioning system, location-aware services, high-resolution remote sensing, and internet-based volunteered geographic information, has resulted in an ever increasing interest in the application of geographic data as well as incorporating spatial information into relevant analysis.

To maintain the privacy of the users, such a group of datasets is anonymized; in other words, every patient's name and numbers are replaced by a randomly acquired ID that is unique on its own before they are transferred to the third party. However, scholars argue that even such methods might not guarantee anonymization and protection of sensitive personal data [20]. The literature affirms that the integration of the known geographic information systems together with social networks has led to what is known as location-based social networks, which are social networks that contain location information in their individual contents. Such capabilities have made real-time urban sensing very much possible. Majumder et al. (2496) outline the privacy issues in IoT health care applications, as summarized in Table 2.

Butpheng et al. (3–5) argue that localization within the adjacent surroundings is never perceived as a privacy threat, since others are usually observed by other people within their individual field of view [1]. However, localization is seen as a large threat, especially when the information is recorded, processed and finally stored without having the permission and control of the subjects in question. As with other concepts of privacy, the absence of control is key to the general concept of privacy location, which is described as the strong ability to prevent some other parties from trying to learn an individual's present or even past location [2].

By the real emergence of the AI-driven IoT, numerous factors could possibly exaggerate the overall privacy threat of the localization because there will be expansion of the possible location-aware applications as well as overall improvements in their accuracy, the overall ubiquity of data collection technology and the whole process involved, and finally, the interaction with the devices for the AI-driven IoT that register the location, identity, and activity of the user. The present studies on location privacy, such as the trusted third party and peer-to-peer aspects, among others, primarily deal with location-aware applications within smartphones and never encompass location privacy threats within the AI-driven IoT. Wang et al. (281) identifies three major challenges: addressing the general threats of a pervasive collection of data, the manner to control the shared location data, and privacy-preserving protocols for proper interaction with the Internet of Things systems [3].

Table 2
Major privacy issues and associated solutions in IoT health care applications.

Privacy issues	IoT-based solutions
PHRS exposure	Encryption before outsourcing, dividing health system into domains, analyzing sensitive data to be private or not.
Cyberattacks	Detection methods and system recovery.
Data eavesdropping and data confidentiality	Data hiding and cryptographic techniques.
Identity threats and privacy of stored data	Pseudonymization of medical data, identity management, anonymity.
Location privacy	Security protocols.

4. Conclusions and recommendations

4.1. Conclusions

Errors made in health care setup are not only costly but also harmful. The literature reports that medical errors are responsible for thousands of deaths annually all over the world, both in developed and developing countries. Regarding a study conducted on 37 million records of patients, approximately 195 thousand people usually die in the United States of America as a result of medical errors committed by clinicians and would easily be prevented. The situation is even worst in developing countries in Africa, where the figure triples at times. It is therefore very clear that powerful clinical decision support systems are needed for the purpose of reducing the time of diagnosis and increasing the accuracy for disease diagnosis. AI-driven IoT has evolved from traditional statistical algorithms to neural networks that are somewhat artificially complex. The usage of tools of data mining and IoT has become commonly used in clinical applications for making health-related decisions in a more effective manner. A number of techniques of data mining, such as decision trees, artificial neural networks, support vector machines, Bayesian networks, and bagging algorithms, have been used widely in clinical support systems for making health-related decisions.

Having a comprehensive knowledge base and advanced functionalities plays an important role in designing an efficient smart health care system. Artificial neural networks and data mining have attracted considerable attention in designing clinical support due to their abilities to discover hidden patterns and relationships in medical data. This paper aims to review the performance of data mining applications in clinical decision support systems and analyze the potential data mining challenges that can support researchers in better understanding of data mining in this area while conducting research in the future.

4.2. Recommendations

It is wise to note that the security and privacy challenges associated with the AI-driven IoT need to be handled on a permanent basis to realize its maturation and growth. First, it is important to acknowledge the fact that AI-driven IoT tends to use varied devices, protocols, and services to realize an intended goal. To integrate the network for the Internet of Things frameworks for the purpose of achieving a greater framework, for instance, to form a smart health care system by integrating several smart hospitals, there is a great need for the establishment of a set of standards that ought to be followed correctly from the micro to the macro levels of realizing the Internet of Things. The current requirements for the Internet of Things are actually to have properly defined architecture standards that include interfaces, data models, and relevant protocols that are able to support a wider range of devices, humans, operating systems, and languages.

Second, there is a need for identity management to solve both the security and privacy risks associated with the AI-driven IoT. Identity management within the Internet of Things can simply be undertaken by trying to exchange identifying relevant information between the things for all of the first-time connections. Such a process can be very susceptible to eavesdropping, which can subsequently result in a type of man-in-the-middle attack and can therefore actually jeopardize the whole framework of the AI-driven IoT. There are therefore some great needs for a type of predefined management entity of an identity or hub that can monitor the overall connection process of the relevant devices through the application of cryptography plus some other relevant techniques, to help prevent the theft of identity.

As outlined by most authors, the three-layer architecture of the AI-driven IoT never accommodates the actual opening, closing and adequate management of a session between the two existing things. There is therefore a great need for protocols that can address all such issues and can eventually ease the mode of communication between the relevant devices. There is a great need to accommodate an abstract session layer as a form of additional layer within the architecture of AI-driven IoT, which is capable of managing protocols, connections, and relevant sessions, which are there between the communications of the relevant heterogeneous devices.

In conclusion, it is evident that the AI-driven IoT frameworks used both in smart medical devices are highly susceptible to different forms of security and privacy threats; therefore, there exist many security and privacy challenges as well as relevant requirements that all must be addressed. The present amount of research carried out on the issues of AI-driven IoT is basically focused on the access and authentication control protocols, although with the advancement of modern technology, it is very important to actually incorporate some other new networking protocols, such as IPv6 and 5G, to realize a dynamic mashup of the Internet of Things topology. The main developments that have been witnessed in the AI-driven IoT are primarily on a smaller scale, such as within small hospitals. For AI-driven IoT to be scaled up, there are several security and privacy concerns that have to be addressed in a proper manner. It is true that AI-driven IoT has a great ability to transform the way in which we live today.

However, the greatest concern in achieving complete smart frameworks is security. In the event that security concerns such as confidentiality, privacy, access control, authentication, end-to-end security, trust management, global standards and relevant policies are completely addressed in the correct manner, it will be very much possible to realize the transformation of almost everything in the health care sector by the IoT within the future to come. There is a great need for new wireless, identification, software and hardware technologies to resolve all of the privacy and security challenges within the IoT, such as the standards for devices that are heterogeneous in nature, trying to implement important management together with identity establishment systems and hubs for trust management. The governance of AI-driven IoT to ensure privacy and security remains the main challenges in the implementation of IoT in both smart homes and medical devices. Implementing a proper governance framework is essential for the success of AI-driven IoT across different aspects of architecture through implementation standards.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The author deeply acknowledges the Researchers Supporting Program (TUMA-Project-2021-14), AlMaarefa University, Riyadh, Saudi Arabia for supporting steps of this work.

Reference

[1] Butpheng C, Yeh K-H, Xiong H. Security and privacy in IoT-cloud-based e-health systems—a comprehensive review. Symmetry Jul. 2020;12(7):1191. https://doi.org/10.3390/sym12071191 [Online]. Available:.

[2] Firouzi F, Farahani B, Barzegari M, Daneshmand M. AI-driven data monetization: the other face of data in IoT-based smart and connected health. In: IEEE Internet Things J.; 2020. https://doi.org/10.1109/JIOT.2020.3027971.

[3] Wang M, Zhu T, Zhang T, Zhang J, Yu S, Zhou W. Security and privacy in 6G networks: new areas and new challenges. Digital Commun Netw 2020;6(3):281–91.

[4] Kim H, Ben-Othman J, Mokdad L, Son J, Li C. Research challenges and security threats to AI-driven 5G virtual emotion applications using autonomous vehicles, drones, and smart devices. 6. In: IEEE network, vol. 34; Nov/Dec 2020. p. 288–94. https://doi.org/10.1109/MNET.011.2000245.

[5] Smith V, Devane D, Begley CM, Clarke M. Methodology in conducting a systematic review of systematic reviews of healthcare interventions. BMC Med Res Methodol 2011;11(1):1–6.

[6] Crowther M, Lim W, Crowther MA. Systematic review and meta-analysis methodology. The Journal of the American Society of Hematology Blood Oct 2010;116(17):3140–6.

[7] Si SL, You XY, Liu HC, Zhang P. DEMATEL technique: a systematic review of the state-of-the-art literature on methodologies and applications. 2018 Math Probl Eng 2018. https://doi.org/10.1155/2018/3696457 [Online], Available:.

[8] James KL, Randall NP, Haddaway NR. A methodology for systematic mapping in environmental sciences. Environ Evid 2016;5(1):1–13.

[9] Munn Z, Peters MD, Stern C, Tufanaru C, McArthur A, Aromataris E. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Med Res Methodol 2018;18(1):1–7.

[10] Sodhro AH, Pirbhulal S, de Albuquerque VHC. Artificial intelligence-driven mechanism for edge computing-based industrial applications. 7. In: IEEE Transactions on Industrial Informatics, vol. 15; July 2019. p. 4235–43.

[11] Garbuio M, Lin N. Artificial intelligence as a growth engine for health care startups: emerging business models. Calif Manag Rev 2019;61(2):59–83.

[12] Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. Academic Press Artificial intelligence in healthcare 2020:295–336.

[13] Nadia-Ghomsheh A, Farahani B, Kavian M. A hierarchical privacy-preserving IoT architecture for vision-based hand rehabilitation assessment. Multimed Tool Appl 2021:1–24. https://doi.org/10.1007/s11042-021-10563-2 [Online], Available:.

[14] Puaschunder JM. The legal and international situation of AI, robotics and big data with attention to healthcare. In: Report on behalf of the European Parliament European liberal Forum; 2019. https://doi.org/10.2139/ssrn.3472885 [Online], Available:.

[15] Fadaeddini A, Majidi B, Eshghi M. Privacy preserved decentralized deep learning: a blockchain based solution for secure ai-driven enterprise. International Congress on High-Performance Computing and Big Data Analysis. Cham: Springer; 2019.

[16] Rayan RA, Christos T, Romash BI. The internet of things for healthcare: applications, selected cases and challenges. IoT in Healthcare and Ambient Assisted Living. Singapore: Springer; 2021. p. 1–15.

[17] Ergen O, Belcastro KD. Ai Driven advanced Internet of Things (Iotx2): the future seems irreversibly connected in medicine. Anatol J Cardiol Oct 2019;22(2):15–7.

[18] Majumder S, Aghayi E, Noferesti M, Memarzadeh-Tehran H, Mondal T, Pang Z, Deen MJ. Smart homes for elderly healthcare—recent advances and research challenges. Sensors 2017;17(11):2496.

[19] Maazouzi F, Zarzour H. AI-driven big healthcare analytics: contributions and challenges. In: *Intelligent analytics with advanced multi-industry applications*, Z. Sun. IGI Global: Papua New Guinea; 2021. p. 172–84.

[20] Choi DH, Shon D. Future changes to smart home based on AAL healthcare service. J Asian Architect Build Eng 2019;18(3):190–9.

[21] Reddy S, Allan S, Coghlan S, Cooper P. A governance model for the application of AI in health care. J Am Med Inf Assoc 2020;27(3):491–7.

[22] Surya L. IoT security techniques based on machine learning: how IoT devices use AI to enhance security. Int J Comput Trends Technol 2021;67.